

# Smart iconography on your wiki

Cindy Cicalese



# Don't Make Me Think!

## Conventions are your friends

One of the best ways to make almost anything easier to grasp in a hurry is to follow the existing conventions—the widely used or standardized design patterns. For example:

- **How things look.** Many elements have a standardized appearance, like the icon that tells you it's a link to a video, the search icon, and the social networking sharing options.



# Iconography - key concepts

- Use icons to represent key concepts in your wiki
- Show these icons on the sidebar or menu as a legend to remind the user what they mean
- Show these icons on the title bar of pages to identify what concepts they identify with
- Show these icons in page text as needed (avoid overuse to create a distraction)
- Show these icons in search results

# Example - EMA wiki

<https://collaborate.mitre.org/ema>

# Use icons to represent key concepts in your wiki



Capabilities



Subcapabilities



Behaviors



Behavior  
Instances



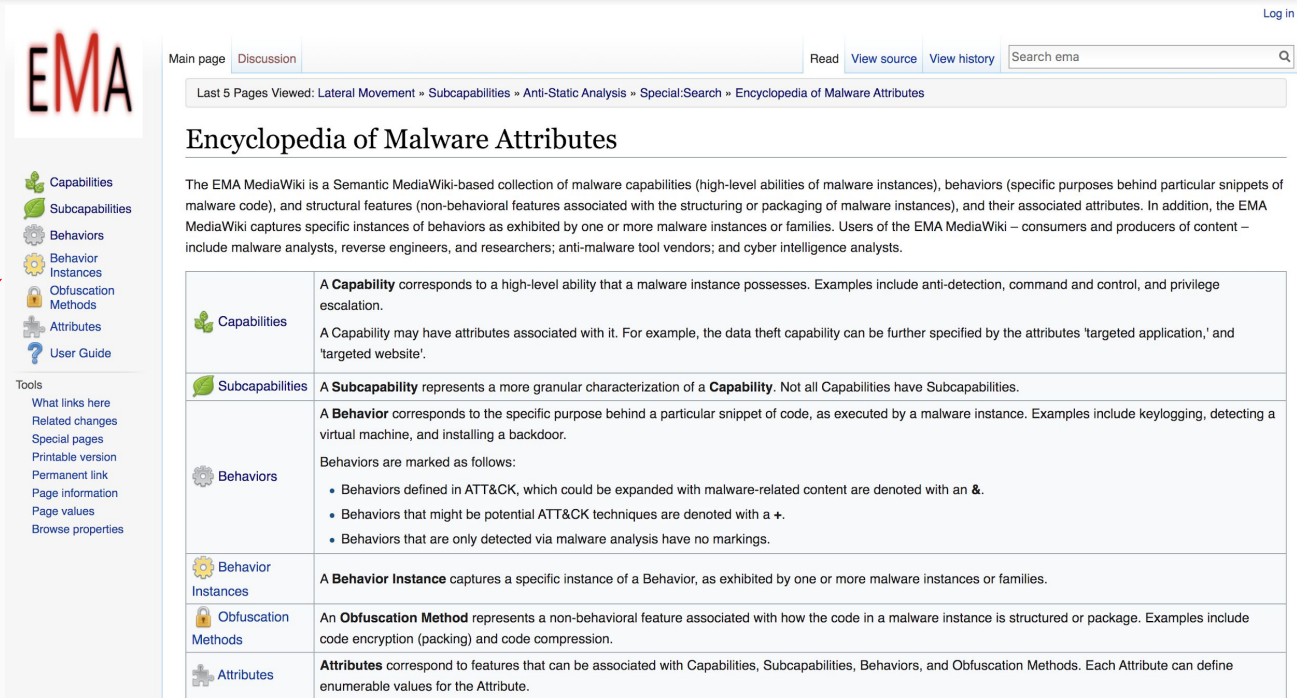
Obfuscation  
Methods









Attributes

# Show these icons on the sidebar or menu as a legend to remind the user what they mean

- example uses extension CustomNavBlocks with Vector skin
- can add icons to menus in Chameleon skin



The screenshot displays the EMA MediaWiki interface. On the left is a sidebar with the EMA logo and a list of categories: Capabilities, Subcapabilities, Behaviors, Behavior Instances, Obfuscation Methods, Attributes, and User Guide. Each category is accompanied by a small icon. Below these is a 'Tools' section with links like 'What links here', 'Related changes', 'Special pages', 'Printable version', 'Permanent link', 'Page information', 'Page values', and 'Browse properties'. The main content area is titled 'Encyclopedia of Malware Attributes' and contains a table with definitions for various terms. The table has two columns: a category name with an icon and a detailed definition.

 Capabilities	<p>A <b>Capability</b> corresponds to a high-level ability that a malware instance possesses. Examples include anti-detection, command and control, and privilege escalation.</p> <p>A Capability may have attributes associated with it. For example, the data theft capability can be further specified by the attributes 'targeted application,' and 'targeted website'.</p>
 Subcapabilities	<p>A <b>Subcapability</b> represents a more granular characterization of a <b>Capability</b>. Not all Capabilities have Subcapabilities.</p>
 Behaviors	<p>A <b>Behavior</b> corresponds to the specific purpose behind a particular snippet of code, as executed by a malware instance. Examples include keylogging, detecting a virtual machine, and installing a backdoor.</p> <p>Behaviors are marked as follows:</p> <ul style="list-style-type: none"><li>• Behaviors defined in ATT&amp;CK, which could be expanded with malware-related content are denoted with an <b>&amp;</b>.</li><li>• Behaviors that might be potential ATT&amp;CK techniques are denoted with a <b>+</b>.</li><li>• Behaviors that are only detected via malware analysis have no markings.</li></ul>
 Behavior Instances	<p>A <b>Behavior Instance</b> captures a specific instance of a Behavior, as exhibited by one or more malware instances or families.</p>
 Obfuscation Methods	<p>An <b>Obfuscation Method</b> represents a non-behavioral feature associated with how the code in a malware instance is structured or package. Examples include code encryption (packing) and code compression.</p>
 Attributes	<p><b>Attributes</b> correspond to features that can be associated with Capabilities, Subcapabilities, Behaviors, and Obfuscation Methods. Each Attribute can define enumerable values for the Attribute.</p>

# Show these icons on the title bar of pages to identify what concepts they identify with



-  Capabilities
-  Subcapabilities
-  Behaviors
-  Behavior Instances
-  Obfuscation Methods
-  Attributes
-  Graph This Page
-  User Guide

Page

Discussion

Read

View form

View history

Search ema

Log in

Last 5 Pages Viewed: [targeted sandbox](#) » [cryptocurrency type](#) » [Attributes](#) » [Graph of](#) » [sandbox detect & evade](#)



## sandbox detect & evade

<b>EMA ID:</b>	ema-1233
	<p>Detects whether the malware instance is being executed inside of an instrumented sandbox environment (e.g., Cuckoo Sandbox). If so, conditional execution selects for benign execution path.</p> <p><b>Examples:</b></p> <ul style="list-style-type: none"><li>• <b>Injected DLL Testing:</b> Testing for the name of a particular DLL that is known to be injected by a sandbox for API hooking is a common way of detecting sandbox environments. This can be achieved through the <code>kernel32!GetModuleHandle</code> API call and other means.</li><li>• <b>Product Key/ID Testing:</b> Checking for a particular product key/ID associated with a sandbox environment (commonly associated with the Windows host OS used in the environment) can be used to detect whether a malware instance is being executed in a particular sandbox. This can be achieved through several means, including testing for the Key/ID</li></ul>

# Show these icons in page text as needed (avoid overuse to create a distraction)



Capabilities



Subcapabilities



Behaviors



Behavior  
Instances



Obfuscation  
Methods



Attributes

[http://unprotect.tdgt.org/index.php/Sandbox\\_Evasion](http://unprotect.tdgt.org/index.php/Sandbox_Evasion)

- Find Agent: Cuckoo uses a python agent to interact with the host guest. By listing the process and finding python.exe or pythonw.exe or by looking for an agent.py in the system, a malware can detect Cuckoo.

[http://unprotect.tdgt.org/index.php/Sandbox\\_Evasion](http://unprotect.tdgt.org/index.php/Sandbox_Evasion)

## Associated Attributes:

Anti-Behavioral Analysis: targeted sandbox, Common: applicable platform, Common: technique

## Associated

## Capabilities/Subcapabilities:



Anti-Behavioral Analysis

## Associated With sandbox detect & evade



Injected DLL Testing



Product Key/ID Testing



Screen Resolution Testing



Timing/Date Checks

## References:

Date	Malware Family	URL
October 23, 2017	Ursnif	<a href="https://securityintelligence.com/news/banking-trojan-uses-malware-macros-to-evade-sandbox-detection/">https://securityintelligence.com/news/banking-trojan-uses-malware-macros-to-evade-sandbox-detection/</a>
January 1, 2014	Terminator	<a href="https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/file/fireeye-hot-knives-through-">https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/pf/file/fireeye-hot-knives-through-</a>



# Show these icons in search results

Capabilities

Subcapabilities

Behaviors

Behavior Instances

Obfuscation Methods

Attributes

User Guide

Tools

Special pages

Printable version

Q sandbox

✕

Search

Results 1 – 12 of 12

Content pages Multimedia Everything Advanced

targeted sandbox

IName=targeted **sandbox** IDescription=The 'targeted **sandbox**' value refers to the name of a **sandbox** targeted by the Anti-Behavioral Analysis Capability.  
232 bytes (29 words) - 18:08, 7 July 2017

sandbox obstruction

IName=**sandbox** obstruction IDescription=The '**sandbox** obstruction' Behavior impedes **sandbox** analysis.  
2 KB (208 words) - 14:35, 3 October 2018

sandbox detect & evade

IName=**sandbox** detect & evade ...being executed inside of an instrumented **sandbox** environment (e.g., Cuckoo **Sandbox**). If so, conditional execution selects for benign execution path.  
4 KB (552 words) - 22:25, 7 October 2018

virtual machine detect & evade

...uman activity, the machine is suspected to be a virtualized machine and/or **sandbox**.  
6 KB (966 words) - 22:25, 7 October 2018

Injected DLL Testing

...n to be injected by a **sandbox** for API hooking is a common way of detecting **sandbox** environments. This can be achieved through the kernel32!GetModuleHandle API  
995 bytes (129 words) - 18:07, 7 July 2017



# TitleIcon

Browse wiki

sandbox detect & evade

Title Icon

Behavior.png + 🔍

[https://www.mediawiki.org/wiki/Extension:Title\\_Icon](https://www.mediawiki.org/wiki/Extension:Title_Icon)

- Use SMW property to specify Title Icon as the name of a File page on a page (possibly in a template) or category
- Image is scaled and displayed on the title bar and in search results
- Can use SMW to query for Title Icon to display in page text

# Potential enhancements to TitleIcon

- alternate storage mechanisms:
  - Multi-content Revisions (MCR)
  - Cargo
- parser function to retrieve icons
- alternate icon types:
  - Unicode characters (<https://phabricator.wikimedia.org/T184134>)
  - Font Awesome icons
  - requires a non-backward compatible change to allow typed icons
- specify link target (<https://phabricator.wikimedia.org/T190822>)
- Title Icons for namespaces (<https://phabricator.wikimedia.org/T190824>)
- merge with DisplayTitle?